ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

Ensuring Data Privacy and Preventing Intrusions in Hospital Data Sharing on Cloudlets

Syed.Karimunnisa[1],

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation Vaddesvaram, Guntur, AP, India-522302,

karimun1.syed@gmail.com

Supriya Menon M[2]

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation Vaddesvaram, Guntur, AP, India-522302,

supriyamenon05@gmail.com

Abstract:

An urge to secure medical data is increasing dramatically, since wearable technology and cloud and cloudlet technologies emerged. The realm of medical data comprises three distinct security challenges: collection, storage, and sharing. Conventional healthcare systems send private patient information to the cloud, which increases communication energy usage. In practice, sharing medical data turns out to be quite difficult. In this paper, we present a novel healthcare system that makes use of cloudlets' flexibility. The cloudlet's features include intrusion detection, data sharing, and privacy protection. During the data collecting stage, we use the Number Theory Research Unit (NTRU) approach to encrypt data that we get from wearable devices. Next, the encrypted data is moved to neighbouring cloudlets. We then develop a novel trust model that allows users to find similar but trustworthy patients who are eager to communicate about their disease and share data that has been kept in the cloudlet. Additionally, the medical data of users is divided into three sections, each of which is securely stored in the cloud of the remote hospital. We integrate a novel cloudlet mesh-based collaborative intrusion detection system (IDS) technique to strengthen the healthcare system against malicious attacks. Our tests validate the effectiveness of the of the proposed scheme.

Keywords: privacy protection, data sharing, collaborative intrusion detection system (IDS), healthcare.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

1. Introduction

Provide As cutting-edge technologies advance, meeting users' ever-increasing demands in cloud-assisted healthcare big data computing has gotten more difficult [3][5]. However, guaranteeing the safety of particular medical data continues to be a challenging problem [6]. Prior initiatives have tracked disease treatment procedures in real-time by utilising social networks and healthcare services [9]. By facilitating access to knowledge from patients who are similar to oneself through shared data, platforms such as Patients Like Me [9] can improve individual findings. Although sharing medical data on social networks has benefits, there are privacy and security risks when doing so [10][11] if appropriate safeguards aren't in place [12]. Large amounts of data storage are currently dispersed among multiple cloud environments [13], including cloudlets [14] and remote clouds [15], which enable data exchange and heavy computations [16][17]

In order to tackle the previously described issues, this study presents a cloudlet-based healthcare system. Information from wearables about users' physiological parameters is sent to local cloudlets and then sent to a remote cloud that doctors can access to diagnose patients.

Vital indicators gathered by wearables are transmitted to a nearby cloudlet gateway in the first phase, with data protection being the main priority. In the second phase, cloudlets transport user data to the remote cloud. A cloudlet, which consists of several mobile devices, takes privacy protection and data sharing into account while meeting owners' demands for particular data contents. In particular, the trust model is applied to evaluate the trustworthiness of users in order to decide which data to provide.

Users' medical data is categorized and subject to certain security standards in order to protect it on the remote cloud. In addition to these three-phase data privacy protocols, a cloudlet mesh-based collaborative intrusion detection system (IDS) is integrated to protect the cloud ecosystem.

2. Related Work

[1] H. Mohamed, L. Adil, T. Saida, and M. Hicham,to address security breaches, a cooperative intrusion system for detecting and avoiding are built on distributed IDS and IPS uses a hybrid detection method. By using the Signature Apriori Algorithm, new attack signatures can be created to help identify and stop different kinds of attacks. By solving attack

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

concerns and creating novel security techniques, the goal is to improve security measures. The author offers a synopsis of cloud computing intrusion detection and suggests a fresh idea for cloud privacy protection.

[11] N.Coa To provide cloud users with a multi-keyword strategy for encrypted data, MRSE (Multikeyword Ranked Search over Encrypted Data in Cloud Computing) was established as a privacy protection solution. Although this method provides users with useful result rating, there may be a significant computational burden associated with it.

[19] R. Lu, X. Lin, and X. Shen,A unique privacy-preserving scalar product computation (PPSPC) technique is integrated with attribute-based access control in the opportunistic computing framework known as SPOC, which focuses on secure and privacy-preserving operations. Medical users are empowered to choose who processes their substantial Personal Health Information (PHI) by using this architecture. The suggested SPOC system successfully assures user-centric privacy access control in emergency m-Healthcare scenarios, according to a thorough security analysis.

3. Methodology

Wearable devices first collect the user's physiological data, which is then sent to a cloudlet. Various concerns of healthcare data protection are considered:

- Ensuring the security of user's physiological data during transit to the cloudlet.
- Guaranteeing that data sharing within the cloudlet doesn't compromise privacy.
- Securing the storage of extensive healthcare data in a remote cloud.
- Effectively fortifying the entire system against malicious attacks?.

With an emphasis on multi-key word ranked search over encrypted data in cloud computing, the current MRSE system seeks to provide users with a multi-keyword approach for encrypted cloud data. But the computational part presents difficulties .

A collaborative system built for cloud environments that makes use of distributed IDS and IPS use a hybrid detection technique to find and stop various types of intrusions that can endanger the system, particularly distributed intrusions. With the use of the cloudlet mesh topology, the collaborative IDS presents a novel intrusion detection method, emphasizing a remarkably high intrusion detection rate. This paper presents a new idea intended to improve

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

privacy protection in the cloud and gives an overview of intrusion detection in cloud computing

Proposed Approach

- We protect users' physiological data while transferring it to cloudlets by using NTRU.
- We can determine whether or not data should be shared in the cloudlet by building a new trust model that assesses user reputation and similarity to determine the trust level.
- We partition the data stored in the remote cloud into various categories and employ distinct encryption mechanisms to protect each category accordingly.
- To defend the entire healthcare system from malicious attacks, we deploy a co-operative Intrusion Detection System (IDS) employing a cloudlet mesh.

System Architecture

The healthcare systems model designed for cloudlet-based system is mentioned as below.

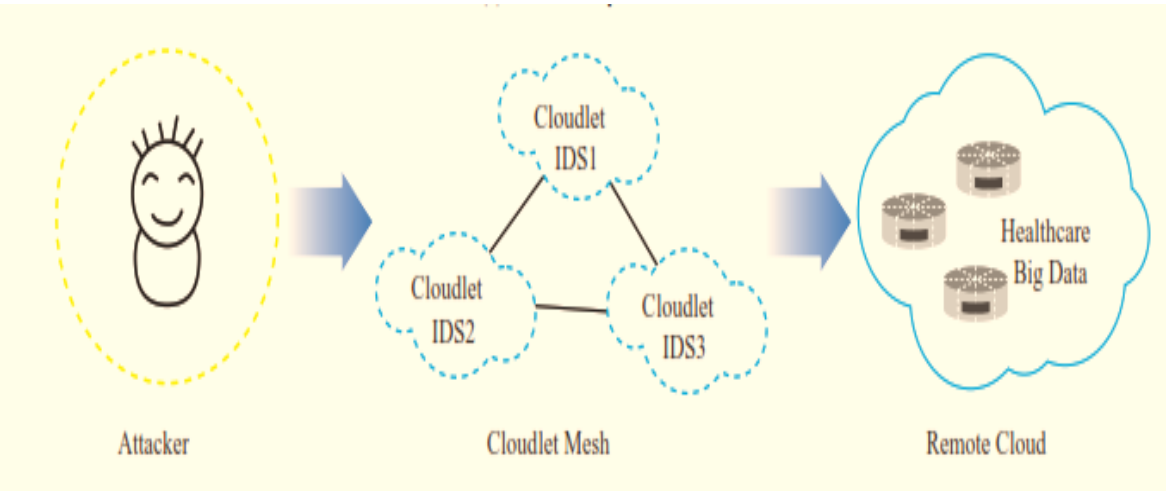

Figure 1 Collaborative IDS of remote cloud

A. Encryption at User End

To protect the privacy of user data and stop private information from being misused or disclosed without authorization during communications.

Step 1: Use wearable technology to collect data.

Step 2: Compute the public and secret keys using the NTRU paradigm.

Step 3: For increased security, encrypt the data using these keys.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

Step 4: Process the data using homomorphic encryption to ensure safe transfer to the cloudlet, saving bandwidth and energy.

B. Medical Data Shared in Cloud

This work addresses the concept of exchanging extensive health related data both at remote clouds and respective cloudlets.

Step 1: When user P intends to exchange data with some user q, the central reliable third-party authority at the hospital looks over user q's data.

Step 2: Using a trusted model, the trusted authority calculates the trust levels of users p and q by assessing their reputation and similarities.

Step 3: The computed trust level is compared with a threshold value determined by the trusted authority.

Step 4: User p may share data with User q if the trust level is at least as high as the threshold value; if not, sharing is prohibited.

Step 5: The Intrusion Detection System (IDS) will sound an alarm if anything is detected.

C. Medical Data Privacy Protection in the Cloud

Step 1: Divide the data into EID, QID, and MI parts.

Step 2: EID includes attributes like name, phone number, and email that are directly linked to the individual. QID consists of attributes such as date of birth and zip code that only partially identify the individual. MI contains details about diseases.

Step 3: Conduct a survey with the individual to get particular information about their illness so that MI can be encrypted.

Step 4: Create questions that match to each trait associated with a particular illness.

Step 5: To make encryption easier, translate these attributes into numerical data that is expressed as 0s and 1s combinations.

Step 6: To protect privacy, encrypt the three sections of the data that are kept in the cloudlet.

D. Collaborative IDS

Step 1: To find intruders inside the system, create a collaborative IDS system using a collection of IDS.

Step 2: Every IDS runs independently to find intrusions.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

Step 3: To prevent malicious attacks, the Collaborative IDS serves as a barrier that screens all database visits.

Step 4: Assess the false alarm and intrusion detection rates.

Step 5: The IDS initiates an alert beforehand to prevent the visit and vice versa if detection indicates a possible malicious attack.

E. Evaluation Of Collaborative IDS

Step 1: There are three sorts of cost issues related to collaborative IDS:

- When the system is unable to identify invasive behaviour, IDS raises an alarm, stopping the transfer of the user's data.
- This intrusive behaviour is made possible by IDS's failure to sound an alarm during system penetration, endangering the large data in healthcare.
- In the other circumstances, the cost is indicated as 0.

Step 2: Assess the anticipated cost by utilizing the Decision tree model.

Step 3: Using a decision tree, formulate an optimisation problem to determine the ideal number of IDS for the system. A common solution such as Matlab can be used to address this problem. By using this method, we want to identify the precise number of IDS systems that ensure: (i) an adequate rate of detection. (ii) a sufficiently low false alarm rate; and (iii) the minimization of the expected cost for the entire system

4. Results and Discussion

We assess the encrypted algorithm's performance by employing the delivery parameter to assess the client's approach of data encryption against techniques preferred at remote cloud.

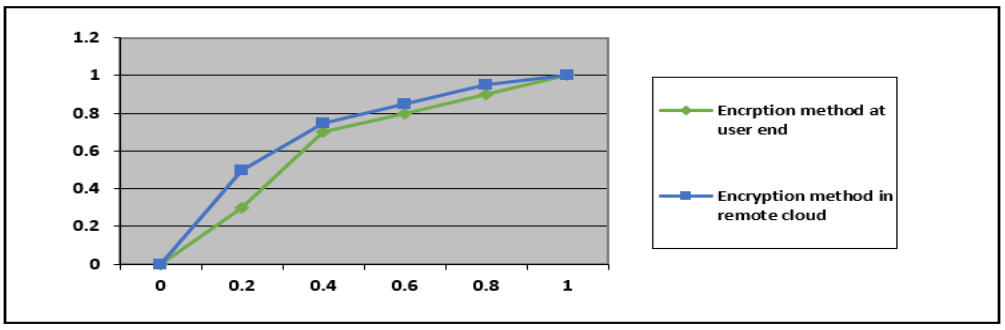

Figure 3 Compare the encryption method's delivery ratio between the user's end and the remote cloud .

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

Using a trust model, we have examined the cloudlet's data sharing schedule

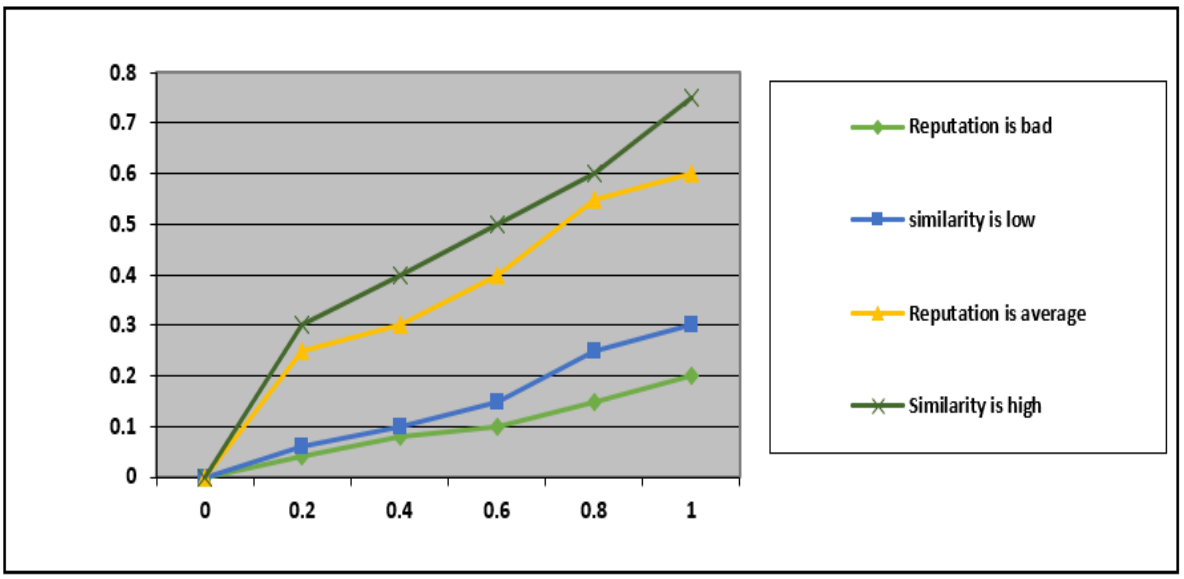

Figure 4 A comparison of the degree of trust

User Reputation and Similarity: We present the ROC curve and the graphical relationship between the number of IDS and their associated costs and detection rates with regard to the collaborative IDS based on the cloudlet mesh.

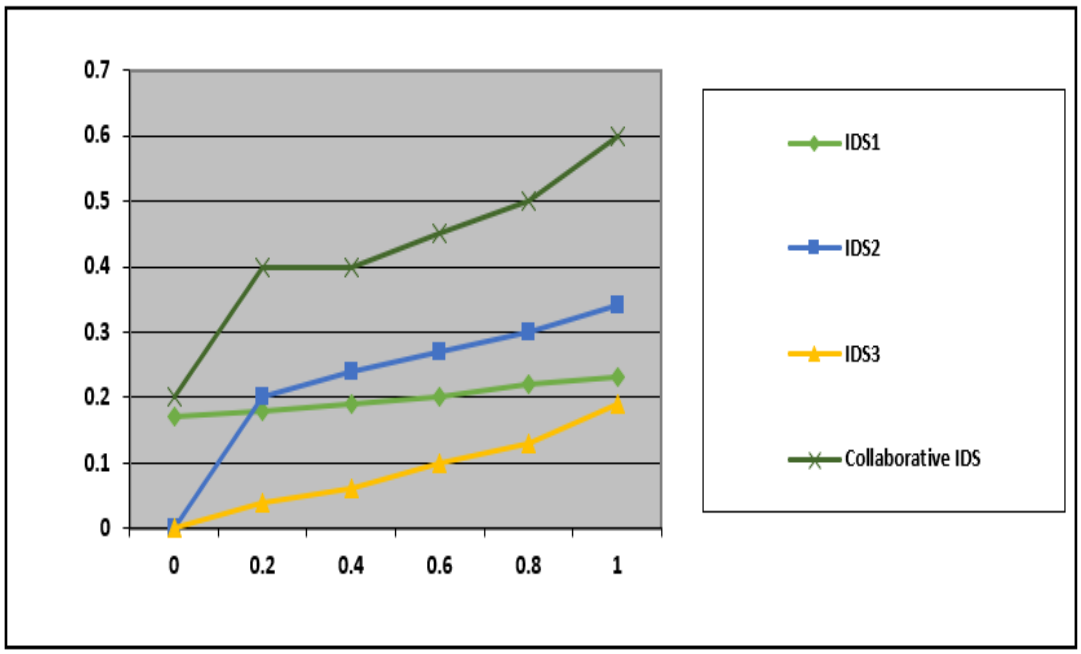

Figure 5 Comparing collaborative IDS's ROC curves.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

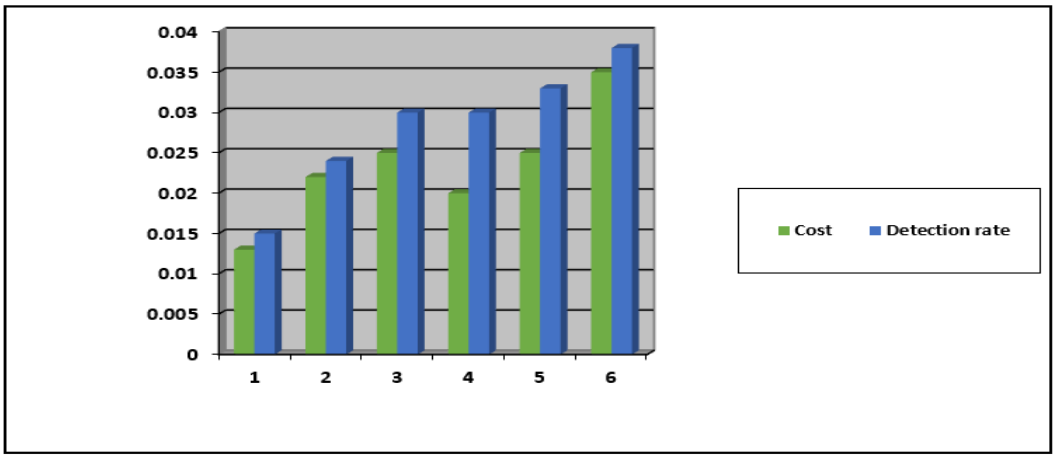

Figure 6 Total IDS system cost and detection rate

4. Conclusions

Exchanging huge amounts of medical related data in the cloud environment and the remote system in cloud is discussed in this study. With the help of our system, users can forward data to the cloudlet, that starts a sharing environment to exchange data at cloudlet. The method consists of multiple steps: Firstly, wearable devices will be used to gather user data, and the NTRU method will be used to ensure that user data is securely transmitted to the cloudlet. Second, evaluating users' trust in order to decide how much data to share in the cloudlet by using a trust model. Third, to safeguard privacy, there are a number of approaches to improve data protection and transmission efficiency when encrypting and partitioning data stored in a remote cloud. Lastly, suggesting a cloudlet mesh-based collaborative intrusion detection system to protect the entire system from harmful attacks. These suggested techniques are validated through simulations and experiments.

References

[1].K. Hung, Y. Zhang, and B. Tai, “Wearable medical devices for telehomehealthcare,”inEngineeringinMedicineandBiologySociety,2004. IEMBS’04. 26th Annual International Conference of the IEEE, vol. 2. IEEE, 2004, pp. 5384–5387.

[2] M. S. Hossain, “Cloud-supported cyber–physical localization framework for patients monitoring,” 2015.

[3] J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Ranjan, J. Kołodziej, A. Streit, and D. Georgakopoulos, “A security framework in g-hadoop for big data computing across

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

distributed cloud data centres," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 994–1007, 2014.

[4] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring," Computer Networks, vol. 101, pp. 192–202, 2016.

[5] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on. IEEE, 2010, pp. 268–275.

[6] K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, "Deypos: Deduplicatable dynamic proof of storage for multi-user environments," 2016.

[7] L.GriffinandE.DeLeastar,"Socialnetworkinghealthcare,"inWearable Micro and Nano Technologies for Personalized Health (pHealth), 2009 6th International Workshop on. IEEE, 2009, pp. 75–78.

[8] W. Xiang, G. Wang, M. Pickering, and Y. Zhang, "Big video data for light-field-based 3d telemedicine," IEEE Network, vol. 30, no. 3, pp. 30– 38, 2016.

[9] https://www.patientslikeme.com/.

[10] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," Network, IEEE, vol. 24, no. 4, pp. 13–18, 2010.

[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[12] K. T. Pickard and M. Swan, "Big desire to share big health data: A shift in consumer attitudes toward personal health information," in 2014 AAAI Spring Symposium Series, 2014.

[13] Y. Shi, S. Abhilash, and K. Hwang, "Cloudlet mesh for securing mobile clouds from intrusions and network attacks," in The Third IEEE International Conference on Mobile Cloud Computing, Services, and Engineering,(Mobile Cloud 2015). IEEE, 2015.

[14] E. Vasilomanolakis, S. Karuppayah, M. M¨uhlh¨auser, and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," ACM Computing Surveys (CSUR), vol. 47, no. 4, p. 55, 2015.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

[15] P. K. Rajendran, B. Muthukumar, and G. Nagarajan, "Hybrid intrusion detection system for private cloud: a systematic approach," Procedia Computer Science, vol. 48, pp. 325–329, 2015.

[16] I.-R. Chen and R. Mitchell "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," Dependable and Secure Computing, IEEE Transactions on, vol. 12, no. 1, pp. 16–30, 2015.

[17] Hsiang-Cheh Huang, Wai-Chi Fang, "Integrity Preservation and Privacy Protection for Medical Images with HistogramBased Reversible Data Hiding", IEEE, 2011.

[18] Tohari Ahmad, HudanStudiawan, HafidhSholihuddin Ahmad, Royyana M. Ijtihadie, WaskithoWibisono, "Shared Secretbased Steganography for Protecting Medical Data" IEEE 2014 International Conference on Computer, Control, Informatics and its Applications, July 2014.

[19] Lingjia Liu, RachadAtat and Yang Yi, "Privacy Protection Scheme for eHealth Systems: A Stochastic Geometry Approach", IEEE, September 2016.

[20] Zhong Han, Yuqing Sun, Yuan Wang, "Audit Recommendation for Privacy Protection in Personal Health Record Systems", Proceedings of the 2013.